

A Class of Three-Weight Cyclic Codes

Zhengchun Zhou and Cunsheng Ding

Abstract

Cyclic codes are a subclass of linear codes and have applications in consumer electronics, data storage systems, and communication systems as they have efficient encoding and decoding algorithms. In this paper, a class of three-weight cyclic codes over $\text{GF}(p)$ whose duals have two zeros is presented, where p is an odd prime. The weight distribution of this class of cyclic codes is settled. Some of the cyclic codes are optimal. The duals of a subclass of the cyclic codes are also studied and proved to be optimal.

Index Terms

Cyclic codes, weight distribution, quadratic form, sphere packing bound.

I. INTRODUCTION

Throughout this paper, let m and k be positive integers such that $s = m/e$ is odd and $s \geq 3$, where $e = \gcd(m, k)$. Let p be an odd prime and $q = p^e$. Let π be a primitive element of the finite field $\text{GF}(q^s)$, where $q^s = p^m$.

An $[n, \ell, d]$ linear code over $\text{GF}(p)$ is an ℓ -dimensional subspace of $\text{GF}(p)^n$ with minimum (Hamming) distance d . Let A_i denote the number of codewords with Hamming weight i in a code C of length n . The weight enumerator of C is defined by

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n.$$

The sequence $(1, A_1, A_2, \dots, A_n)$ is called the weight distribution of the code C .

An $[n, \ell]$ linear code C over the finite field $\text{GF}(p)$ is called cyclic if $(c_0, c_1, \dots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$. By identifying the vector $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(p)^n$ with

$$c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \text{GF}(p)[x]/(x^n - 1),$$

any code C of length n over $\text{GF}(p)$ corresponds to a subset of $\text{GF}(p)[x]/(x^n - 1)$. The linear code C is cyclic if and only if the corresponding subset in $\text{GF}(p)[x]/(x^n - 1)$ is an ideal of the polynomial residue class ring $\text{GF}(p)[x]/(x^n - 1)$. It is well known that every ideal of $\text{GF}(p)[x]/(x^n - 1)$ is principal. Let $C = (g(x))$, where $g(x)$ is monic and has the least degree. Then $g(x)$ is called the generator polynomial and $h(x) = (x^n - 1)/g(x)$ is referred to as the parity-check polynomial of C . A cyclic code is called irreducible if its parity-check polynomial is irreducible over $\text{GF}(p)$. Otherwise, it is called reducible.

The weight distributions of both irreducible and reducible cyclic codes have been interesting subjects of study for many years. For information on the weight distribution of irreducible cyclic codes, the reader is referred to [18], [23], [19], and the recent survey [6]. Information on the weight distribution of reducible cyclic codes could be found in [21], [7], [14], [15], [5], [16], and [22].

Let $h_0(x)$, $h_1(x)$, and $h_2(x)$ be the minimal polynomials of π^{-1} , $(-\pi)^{-1}$, and $\pi^{-(p^k+1)/2}$ over $\text{GF}(p)$, respectively. It is easy to show that $h_0(x)$, $h_1(x)$, and $h_2(x)$ are polynomials of degree m and are pairwise

Z. Zhou's research was supported by the Natural Science Foundation of China, Proj. No. 61201243. C. Ding's research was supported by The Hong Kong Research Grants Council, Proj. No. 600812.

Z. Zhou is with the School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China (email: zzc@home.swjtu.edu.cn).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (email: cding@ust.hk).

distinct. The cyclic code over $\text{GF}(p)$ with length $p^m - 1$ and parity-check polynomial $h_0(x)h_2(x)$ has been extensively studied and is a three-weight code in the following cases.

- When k is even and $e = 1$, this three-weight cyclic code is due to Trachtenberg [20].
- When k is odd, $e = 1$, and $p = 3$, the cyclic code is related to some planar functions and is proved to have only three nonzero weights by Yuan, Carlet, and Ding [3], [21].
- When k and e are odd and p is any odd prime, Luo and Feng [14] proved that the code has only three nonzero weights.

The objective of this paper is to study the cyclic code over $\text{GF}(q)$ with length $p^m - 1$ and parity-check polynomial $h_1(x)h_2(x)$. It will be shown that this cyclic code has only three nonzero weights when k/e is odd, or k is even and e is odd. The weight distribution of the proposed cyclic codes will be determined. Some of the cyclic codes with parity-check polynomials $h_1(x)h_2(x)$ are optimal. The duals of a subclass of the cyclic codes are also optimal. The three-weight cyclic codes dealt with in this paper may have applications in association schemes [2] and secret sharing schemes [3].

This paper is organized as follows. Section II introduces necessary results on quadratic forms that will be needed later in this paper. Section III defines the class of cyclic codes and determines their weight distributions. Section IV studies the duals of a subclass of the cyclic codes. Section V concludes this paper and makes some comments on this topic.

II. QUADRATIC FORMS OVER FINITE FIELDS

In this section, we give a brief introduction to the theory of quadratic forms over finite fields which is needed to calculate the weight distribution of the cyclic codes in the sequel. Quadratic forms have been well studied (see the monograph [17] and the references therein), and have applications in sequence design ([20], [11]), and coding theory ([7], [14], [15]).

Identifying $\text{GF}(q^s)$ with the s -dimensional $\text{GF}(q)$ -vector space $\text{GF}(q)^s$, a function Q from $\text{GF}(q^s)$ to $\text{GF}(q)$ can be regarded as an s -variable polynomial on $\text{GF}(q)$. The former is called a quadratic form over $\text{GF}(q)$ if the latter is a homogeneous polynomial of degree two in the form

$$Q(x_1, x_2, \dots, x_s) = \sum_{1 \leq i \leq j \leq s} a_{ij} x_i x_j$$

where $a_{ij} \in \text{GF}(q)$, and we use a basis $\{\beta_1, \beta_2, \dots, \beta_s\}$ of $\text{GF}(q^s)$ over $\text{GF}(q)$ and identify $x = \sum_{i=1}^s x_i \beta_i$ with the vector $(x_1, x_2, \dots, x_s) \in \text{GF}(q)^s$. The rank of the quadratic form $Q(x)$ is defined as the codimension of the $\text{GF}(q)$ -vector space

$$V = \{x \in \text{GF}(q^s) \mid Q(x+z) - Q(x) - Q(z) = 0 \text{ for all } z \in \text{GF}(q^s)\}.$$

That is $|V| = q^{s-r}$ where r is the rank of $Q(x)$.

For a quadratic form $f(x)$ in s variables over $\text{GF}(q)$, there exists a symmetric matrix A of order s over $\text{GF}(q)$ such that $f(x) = XAX'$, where $X = (x_1, \dots, x_s) \in \text{GF}(q)^s$ and X' denotes the transpose of X . For a symmetric matrix A of order s over $\text{GF}(q)$, it is known that there is a nonsingular matrix T of order s such that TAT' is a diagonal matrix [17]. Under the nonsingular linear substitution $X = ZT$ with $Z = (z_1, z_2, \dots, z_s) \in \text{GF}(q)^s$, we then have

$$f(x) = ZTAT'Z' = \sum_{i=1}^r d_i z_i^2 \quad (1)$$

where r is the rank of $f(x)$ and $d_i \in \text{GF}(q)^*$. Let $\Delta = d_1 d_2 \dots d_r$ for $r \geq 1$ and $\Delta = 1$ for $r = 0$. Let η_1 denote the quadratic multiplicative character of $\text{GF}(q)$. Then $\eta_1(\Delta)$ is an invariant of A under the conjugate action of $\mathcal{M} \in \text{GL}_s(\text{GF}(q))$. The following results are useful in the sequel.

Lemma 2.1: ([17], [15]) With the notations as above, we have

$$\sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(f(x))} = \begin{cases} \eta_1(\Delta) q^{s-r/2}, & \text{if } q \equiv 1 \pmod{4}, \\ \eta_1(\Delta) (\sqrt{-1})^r q^{s-r/2}, & \text{if } q \equiv 3 \pmod{4} \end{cases}$$

for any quadratic form $f(x)$ in s variables of rank r over $\text{GF}(q)$, where ζ_p is a primitive p -th root of unity, and $\text{Tr}_{q/p}(x)$ denotes the trace function from $\text{GF}(q)$ to $\text{GF}(p)$.

Lemma 2.2: Let $f(x)$ be a quadratic form in s variables of rank r over $\text{GF}(q)$.

- If r is even, then

$$\sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(yf(x))} = \pm(p-1)q^{s-r/2}.$$

- If r and e are odd, then

$$\sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(yf(x))} = 0.$$

Proof: By a nonsingular linear substitution as in (1), we have $f(x) = \sum_{i=1}^r d_i z_i^2$, where $d_i \in \text{GF}(q)^*$ and $(z_1, z_2, \dots, z_r) \in \text{GF}(q)^r$. Note that, for each $y \in \text{GF}(p)^*$, $yf(x)$ is a quadratic form over $\text{GF}(q)$ with rank r and $yf(x) = \sum_{i=1}^r (yd_i)z_i^2$. According to Lemma 2.1, we have

$$\sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(yf(x))} = \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(f(x))} \sum_{y \in \text{GF}(p)^*} \eta_1(y^r).$$

Thus, when r is even,

$$\sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(yf(x))} = \pm(p-1)q^{s-r/2}.$$

On the other hand, when r and e are both odd,

$$\begin{aligned} & \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(yf(x))} \\ &= \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(f(x))} \sum_{y \in \text{GF}(p)^*} \eta_1(y^r) \\ &= \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(f(x))} \sum_{y \in \text{GF}(p)^*} \eta_1(y) \\ &= \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(f(x))} \sum_{y \in \text{GF}(p)^*} \eta_0(y) \\ &= 0 \end{aligned}$$

where η_0 is the quadratic multiplicative character of $\text{GF}(p)$ and in the third identity we used the fact that $\eta_0(x) = \eta_1(x)$ for any $x \in \text{GF}(p)^*$ since e is odd. ■

III. THE CLASS OF THREE-WEIGHT CYCLIC CODES AND THEIR WEIGHT DISTRIBUTION

We follow the notations fixed in Section I. From now on, we always assume that λ is a fixed nonsquare in $\text{GF}(q)$. Note that s is odd, thus λ is also a nonsquare in $\text{GF}(q^s)$. Let SQ denote the set of all squares in $\text{GF}(q^s)^*$. Then λx runs through all nonsquares in $\text{GF}(q^s)$ as x runs through SQ . The following result is easy to prove and is useful in the sequel.

Proposition 3.1: $\lambda^{(1+p^k)/2} = \lambda$ if k/e is even, and $\lambda^{(1+p^k)/2} = -\lambda$ otherwise.

By Delsarte's Theorem [4], the code \mathcal{C} with the parity-check polynomial $h_1(x)h_2(x)$ can be expressed as

$$\mathcal{C} = \{\mathbf{c}_{(a,b)} | a, b \in \text{GF}(q^s)\} \quad (2)$$

where

$$\mathbf{c}_{(a,b)} = \left(\text{Tr}_{q^s/p} \left(a(-\pi)^t + b\pi^{(p^k+1)t/2} \right) \right)_{t=0}^{q^s-2}.$$

In terms of exponential sums, the weight of the codeword $\mathbf{c}_{(a,b)} = (c_0, c_1, \dots, c_{q^s-2})$ in \mathcal{C} is given by

$$\begin{aligned} \text{WT}(\mathbf{c}_{(a,b)}) &= \#\{0 \leq t \leq q^s - 2 : c_t \neq 0\} \\ &= q^s - 1 - \frac{1}{p} \sum_{t=0}^{q^s-2} \sum_{y \in \text{GF}(p)} \zeta_p^{yc_t} \\ &= q^s - 1 - \frac{1}{p} \sum_{y \in \text{GF}(p)} \sum_{t=0}^{(q^s-3)/2} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a \pi^{2t} + y b (\pi^{2t})^{(p^k+1)/2})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \pi \pi^{2t} + y b (\pi \pi^{2t})^{(p^k+1)/2})} \right) \\ &= q^s - 1 - \frac{1}{p} \sum_{y \in \text{GF}(p)} \sum_{x \in \text{SQ}} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a x + y b x^{(p^k+1)/2})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \pi x + y b (\pi x)^{(p^k+1)/2})} \right) \\ &= q^s - 1 - \frac{1}{p} \sum_{y \in \text{GF}(p)} \sum_{x \in \text{SQ}} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a x + y b x^{(p^k+1)/2})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \lambda x + y b (\lambda x)^{(p^k+1)/2})} \right) \\ &= q^s - 1 - \frac{1}{2p} \sum_{y \in \text{GF}(p)} \sum_{x \in \text{GF}(q^s)^*} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a x^2 + y b x^{p^k+1})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \lambda x^2 + y b \lambda^{(p^k+1)/2} x^{p^k+1})} \right) \\ &= p^m - p^{m-1} - \frac{1}{2p} \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a x^2 + y b x^{p^k+1})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \lambda x^2 + y b \lambda^{(p^k+1)/2} x^{p^k+1})} \right) \end{aligned}$$

where in the fifth identity we used the fact that both πx and λx run through all nonsquares in $\text{GF}^*(q^s)$ as x runs through SQ. It then follows from Proposition 3.1 that

- when k/e is even,

$$\text{WT}(\mathbf{c}_{(a,b)}) = p^m - p^{m-1} - \frac{1}{2p} S(a, b)$$

where

$$S(a, b) = \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a x^2 + y b x^{p^k+1})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \lambda x^2 + y b \lambda x^{p^k+1})} \right); \quad (3)$$

- when k/e is odd,

$$\text{WT}(\mathbf{c}_{(a,b)}) = p^m - p^{m-1} - \frac{1}{2p} T(a, b)$$

where

$$T(a, b) = \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \left(\zeta_p^{\text{Tr}_{q^s/p}(y a x^2 + y b x^{p^k+1})} + \zeta_p^{\text{Tr}_{q^s/p}(-y a \lambda x^2 - y b \lambda x^{p^k+1})} \right). \quad (4)$$

Based on the discussions above, the weight distribution of the code \mathcal{C} is completely determined by the value distribution of $S(a, b)$ and $T(a, b)$. To calculate the value distribution of $S(a, b)$ and $T(a, b)$, we need a series of lemmas. Before introducing them, we define

$$\mathcal{Q}_{a,b}(x) = \text{Tr}_{q^s/q}(a x^2 + b x^{1+p^k}), \quad x \in \text{GF}(q^s). \quad (5)$$

for each $(a, b) \in \text{GF}(q^s)^2$.

Lemma 3.2: ([7], [15]) For any $(a, b) \in \text{GF}(q^s)^2 \setminus \{(0, 0)\}$, the function $Q_{a,b}$ of (5) is a quadratic form over $\text{GF}(q)$ with rank $s, s-1$, or $s-2$.

Lemma 3.3: Let k be even and e be odd, and let $S(a, b)$ be defined by (3). Then for any $(a, b) \neq (0, 0)$, $S(a, b)$ takes on only the values from the set $\{0, \pm(p-1)p^{(m+e)/2}\}$.

Proof: According to the definition of $S(a, b)$, we have

$$S(a, b) = \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \left(\zeta_p^{\text{Tr}_{q/p}(yQ_{a,b}(x))} + \zeta_p^{\text{Tr}_{q/p}(y\lambda Q_{-a,b}(x))} \right)$$

where $Q_{a,b}(x)$ is given by (5). We now prove that at least one of the quadratic forms $Q_{a,b}$ and $Q_{-a,b}$ has rank s . When $b = 0$, it is easy to check that both $Q_{a,b}$ and $Q_{-a,b}$ have rank s for any nonzero a . When $b \neq 0$, suppose on the contrary that both $Q_{a,b}$ and $Q_{-a,b}$ have rank less than m . Then there are two nonzero elements $x_1, x_2 \in \text{GF}(q^s)$ such that

$$Q_{a,b}(x_1 + z) - Q_{a,b}(x_1) - Q_{a,b}(z) = 0, \quad \forall z \in \text{GF}(q^s) \quad (6)$$

and

$$Q_{-a,b}(x_2 + z) - Q_{-a,b}(x_2) - Q_{-a,b}(z) = 0, \quad \forall z \in \text{GF}(q^s). \quad (7)$$

Note that

$$Q_{a,b}(x + z) - Q_{a,b}(x) - Q_{a,b}(z) = \text{Tr}_{q^s/q}(z(2ax + bx^{p^k} + b^{p^{-k}}x^{p^{-k}})).$$

It then follows from (6) and (7), respectively, that

$$b^{p^k}x_1^{p^{2k}} + 2a^{p^k}x_1^{p^k} + bx_1 = 0$$

and

$$b^{p^k}x_2^{p^{2k}} - 2a^{p^k}x_2^{p^k} + bx_2 = 0.$$

Combining these two equations (the first one times $x_2^{p^k}$ plus the second one times $x_1^{p^k}$) leads to

$$u(u^{p^k-1} + 1) = 0 \quad (8)$$

where

$$u = bx_1x_2(x_1^{p^k-1} + x_2^{p^k-1}).$$

Note that $x^{p^k-1} \neq -1$ for any $x \in \text{GF}(q^s)^*$ since k/e is even and s is odd. It then follows that $u \neq 0$ and $u^{p^k-1} + 1 \neq 0$. This is a contradiction with (8). Thus at least one of the quadratic forms $Q_{a,b}$ and $Q_{-a,b}$ has rank s for any $(a, b) \neq (0, 0)$. On the other hand, by Lemma 2.2, $S(a, b) \neq 0$ only if $Q_{a,b}$ or $Q_{-a,b}$ has even rank. Thus, $S(a, b) = \pm(p-1)p^{(m+e)/2}$ if $Q_{a,b}$ has rank s and $Q_{-a,b}$ has rank $s-1$ or $Q_{a,b}$ has rank $s-1$ and $Q_{-a,b}$ has rank s , and otherwise $S(a, b) = 0$. This completes the proof. ■

Theorem 3.4: Let k be even and e be odd. Then the value distribution of $S(a, b)$ in (3) is given by

$2(p-1)p^m$	occurring	1	time
$(p-1)p^{(m+e)/2}$	occurring	$(p^{m-e} + p^{(m-e)/2})(p^m - 1)$	times
$-(p-1)p^{(m+e)/2}$	occurring	$(p^{m-e} - p^{(m-e)/2})(p^m - 1)$	times
0	occurring	$(p^m - 2p^{m-e} + 1)(p^m - 1)$	times.

Proof: It is clear that $S(0, 0) = 2(p-1)p^m$. According to Lemma 3.3, we define

$$N_\varepsilon = \#\{(a, b) \in \text{GF}(q^s)^2 \setminus (0, 0) \mid S(a, b) = \varepsilon(p-1)p^{(m+e)/2}\}$$

where $\varepsilon = \pm 1$. Then we have

$$\sum_{a,b} S(a,b) = 2(p-1)p^m + (N_1 - N_{-1})(p-1)p^{(m+e)/2} \quad (9)$$

and

$$\sum_{a,b} S^2(a,b) = 4(p-1)^2 p^{2m} + (N_1 + N_{-1})(p-1)^2 p^{m+e}. \quad (10)$$

On the other hand, it follows from (3) that

$$\sum_{a,b} S(a,b) = 2(p-1)p^{2m} \quad (11)$$

and

$$\sum_{a,b} S^2(a,b) = p^{2m}(\#S_1 + \#S_2 + \#S_3 + \#S_4) \quad (12)$$

where

$$\begin{aligned} S_1 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid y_1 x_1^2 - y_2 x_2^2 = 0, \quad y_1 x_1^{p^k+1} - y_2 x_2^{p^k+1} = 0\}, \\ S_2 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid y_1 x_1^2 + \lambda y_2 x_2^2 = 0, \quad y_1 x_1^{p^k+1} - \lambda y_2 x_2^{p^k+1} = 0\}, \\ S_3 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid -\lambda y_1 x_1^2 - y_2 x_2^2 = 0, \quad \lambda y_1 x_1^{p^k+1} - y_2 x_2^{p^k+1} = 0\}, \\ S_4 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid -\lambda y_1 x_1^2 + \lambda y_2 x_2^2 = 0, \quad \lambda y_1 x_1^{p^k+1} - \lambda y_2 x_2^{p^k+1} = 0\}. \end{aligned}$$

Herein, $\Gamma = \text{GF}(p)^* \times \text{GF}(p)^* \times \text{GF}(q^s) \times \text{GF}(q^s)$. It is not hard to prove that

$$\#S_1 = \#S_4 = (p-1)^2 p^m \quad (13)$$

and

$$\#S_2 = \#S_3 = (p-1)^2. \quad (14)$$

Combining Equations (9)–(14), we get

$$\begin{aligned} N_1 &= (p^{m-e} + p^{(m-e)/2})(p^m - 1), \\ N_{-1} &= (p^{m-e} - p^{(m-e)/2})(p^m - 1). \end{aligned}$$

Summarizing the discussion above completes the proof of this theorem. ■

Lemma 3.5: Let k/e be odd and $T(a,b)$ be defined by (4). Then for any $(a,b) \in \text{GF}(q^s)^2 \setminus \{(0,0)\}$, $T(a,b)$ takes on only the values from the set $\{0, \pm 2(p-1)p^{(m+e)/2}\}$.

Proof: According to the definition of $T(a,b)$, we have

$$T(a,b) = \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q^s)} \left(\zeta_p^{\text{Tr}_{q/p}(yQ_{a,b}(x))} + \zeta_p^{\text{Tr}_{q/p}(-y\lambda Q_{a,b}(x))} \right)$$

where $Q_{a,b}(x)$ is given by (5). By Lemma 3.2, for any $(a,b) \neq (0,0)$, the possible rank of $Q_{a,b}(x)$ is $s, s-1$, or $s-2$. Note that, for any $y \in \text{GF}(p)^*$, the quadratic forms $yQ_{a,b}(x)$ and $-\lambda yQ_{a,b}(x)$ have the same rank with $Q_{a,b}(x)$. When $Q_{a,b}(x)$ has even rank $s-1$, by Lemma 2.2, we have $T(a,b) = \pm 2(p-1)p^{(m+e)/2}$. When $Q_{a,b}(x)$ has odd rank s or $s-2$, we distinguish between the following two cases to show that $T(a,b) = 0$. Case 1: e is odd. In this case, it follows again from Lemma 2.2 that $T(a,b) = 0$. Case 2: e

is even. In this case, -1 is a square in $\text{GF}(q)$ and thus $-\lambda$ is a nonsquare in $\text{GF}(q)$. It then follows from Lemma 2.1 that

$$\begin{aligned} & \sum_{x \in \text{GF}(q^s)} \left(\zeta_p^{\text{Tr}_{q/p}(yQ_{a,b}(x))} + \zeta_p^{\text{Tr}_{q/p}(-y\lambda Q_{a,b}(x))} \right) \\ &= (\eta_1(y) + \eta_1(-y\lambda)) \sum_{x \in \text{GF}(q^s)} \zeta_p^{\text{Tr}_{q/p}(Q_{a,b}(x))} \\ &= 0 \end{aligned}$$

for any $y \in \text{GF}(p)^*$. Thus $T(a, b) = 0$. This completes the proof. \blacksquare

Theorem 3.6: Let k/e be odd. Then the value distribution of $T(a, b)$ in (4) is given by

$2(p-1)p^m$	occurring	1	time
$2(p-1)p^{(m+e)/2}$	occurring	$\frac{1}{2}(p^{m-e} + p^{(m-e)/2})(p^m - 1)$	times
$-2(p-1)p^{(m+e)/2}$	occurring	$\frac{1}{2}(p^{m-e} - p^{(m-e)/2})(p^m - 1)$	times
0	occurring	$(p^m - p^{m-e} + 1)(p^m - 1)$	times.

Proof: It is clear that $T(0, 0) = 2(p-1)p^m$. According to Lemma 3.5, we define

$$n_\varepsilon = \#\{(a, b) \in \text{GF}(q^s)^2 \setminus (0, 0) \mid T(a, b) = 2\varepsilon(p-1)p^{(m+e)/2}\}$$

where $\varepsilon = \pm 1$. Then we have

$$\sum_{a,b} T(a, b) = 2(p-1)p^m + 2(n_1 - n_{-1})(p-1)p^{(m+e)/2} \quad (15)$$

and

$$\sum_{a,b} T^2(a, b) = 4(p-1)^2 p^{2m} + 4(n_1 + n_{-1})(p-1)^2 p^{m+e}. \quad (16)$$

On the other hand, it follows from (4) that

$$\sum_{a,b} T(a, b) = 2(p-1)p^{2m} \quad (17)$$

and

$$\sum_{a,b} T^2(a, b) = p^{2m}(\#T_1 + \#T_2 + \#T_3 + \#T_4) \quad (18)$$

where

$$\begin{aligned} T_1 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid y_1 x_1^2 - y_2 x_2^2 = 0, \quad y_1 x_1^{p^k+1} - y_2 x_2^{p^k+1} = 0\}, \\ T_2 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid y_1 x_1^2 + \lambda y_2 x_2^2 = 0, \quad y_1 x_1^{p^k+1} + \lambda y_2 x_2^{p^k+1} = 0\}, \\ T_3 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid -\lambda y_1 x_1^2 - y_2 x_2^2 = 0, \quad -\lambda y_1 x_1^{p^k+1} - y_2 x_2^{p^k+1} = 0\}, \\ T_4 &= \{(y_1, y_2, x_1, x_2) \in \Gamma \mid -\lambda y_1 x_1^2 + \lambda y_2 x_2^2 = 0, \quad -\lambda y_1 x_1^{p^k+1} + \lambda y_2 x_2^{p^k+1} = 0\}. \end{aligned}$$

Herein, $\Gamma = \text{GF}(p)^* \times \text{GF}(p)^* \times \text{GF}(q^s) \times \text{GF}(q^s)$. It is not hard to show that

$$\#T_1 = \#T_2 = \#T_3 = \#T_4 = (p-1)^2 p^m. \quad (19)$$

Combining Equations (15)–(19), we get

$$\begin{aligned} n_1 &= \frac{1}{2}(p^{m-e} + p^{(m-e)/2})(p^m - 1), \\ n_{-1} &= \frac{1}{2}(p^{m-e} - p^{(m-e)/2})(p^m - 1). \end{aligned}$$

TABLE I
WEIGHT DISTRIBUTION OF C FOR EVEN k AND ODD e

Hamming Weight	Frequency
0	1
$p^m - p^{m-1} - \frac{p-1}{2}p^{(m+e-2)/2}$	$(p^{m-e} + p^{(m-e)/2})(p^m - 1)$
$p^m - p^{m-1}$	$(p^m - 2p^{m-e} + 1)(p^m - 1)$
$p^m - p^{m-1} + \frac{p-1}{2}p^{(m+e-2)/2}$	$(p^{m-e} - p^{(m-e)/2})(p^m - 1)$

TABLE II
WEIGHT DISTRIBUTION OF C FOR ODD k/e

Hamming Weight	Frequency
0	1
$p^m - p^{m-1} - (p-1)p^{(m+e-2)/2}$	$\frac{1}{2}(p^{m-e} + p^{(m-e)/2})(p^m - 1)$
$p^m - p^{m-1}$	$(p^m - p^{m-e} + 1)(p^m - 1)$
$p^m - p^{m-1} + (p-1)p^{(m+e-2)/2}$	$\frac{1}{2}(p^{m-e} - p^{(m-e)/2})(p^m - 1)$

The value distribution of $T(a, b)$ follows from the discussion above. ■

Theorem 3.7: Let k be even and e be odd. Then the code C is a three-weight p -ary cyclic code with parameters $[p^m - 1, 2m, p^m - p^{m-1} - \frac{p-1}{2}p^{(m+e-2)/2}]$. Moreover the weight distribution of C is given in Table I.

Proof: The length and dimension of C follow directly from its definition. The minimal distance and weight distribution of C follow from Equation (3) and Theorem 3.4. ■

The following are some examples of the codes.

Example 3.8: Let $p = 3$ and $m = 3$, and $k = 2$. Then the code C is a $[26, 6, 15]$ code over $\text{GF}(3)$ with the weight enumerator

$$1 + 312x^{15} + 260x^{18} + 156x^{21}.$$

It has the same parameters with the best known cyclic codes in the Database of best linear codes known maintained by Markus Grassl at <http://www.codetables.de/>. It is also optimal since the upper bound is 15.

Example 3.9: Let $p = 3$, $m = 5$ and $k = 4$. Then the code C is a $[242, 6, 153]$ code over $\text{GF}(3)$ with the weight enumerator

$$1 + 21780x^{153} + 19844x^{162} + 17424x^{171}.$$

It has the same parameters with the best known cyclic codes in the Database. It is optimal or almost optimal since the upper bound on the minimal distance of any ternary linear code with length 242 and dimension 6 is 154.

Example 3.10: Let $p = 5$, $m = 3$, and $k = 2$. Then the code C is a $[124, 6, 90]$ code over $\text{GF}(5)$ with the weight enumerator

$$1 + 3720x^{90} + 9424x^{100} + 2480x^{110}.$$

The best known linear code over $\text{GF}(5)$ with length 124 and dimension 6 has minimal distance 95.

Theorem 3.11: Let k/e be odd. Then the code C is a three-weight p -ary cyclic code with parameters $[p^m - 1, 2m, p^m - p^{m-1} - (p-1)p^{(m+e-2)/2}]$. Moreover the weight distribution of C is given in Table II.

Proof: The length and dimension of C follow directly from its definition. The minimal distance and weight distribution of C follow from Equation (4) and Theorem 3.6. ■

Example 3.12: Let $p = 3$ and $m = 6$, and $k = 2$. Then the code C is a $[728, 12, 432]$ code over $\text{GF}(3)$ with the weight enumerator

$$1 + 32760x^{432} + 472472x^{486} + 26208x^{540}.$$

Example 3.13: Let $p = 5$ and $m = 3$, and $k = 1$. Then the code C is a $[124, 6, 80]$ code over $\text{GF}(5)$ with the weight enumerator

$$1 + 1860x^{80} + 12524x^{100} + 1240x^{120}.$$

Example 3.14: Let $p = 3$ and $m = 9$, and $k = 3$. Then the code C is a $[19682, 18, 12879]$ code over $\text{GF}(3)$ with the weight enumerator

$$1 + 7439796x^{12636} + 373072310x^{13122} + 6908382x^{13608}.$$

IV. THE DUALS OF A SUBCLASS OF THE CYCLIC CODES

In this section, we study the duals of a subclass of the cyclic codes presented in this paper and prove that they are optimal ternary linear codes.

Theorem 4.1: Let $p = 3$, k be even and e be odd. Then the dual C^\perp of the cyclic code C in (2) is an optimal ternary code with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.

Proof: We only need to prove that C^\perp has minimal distance 4. Clearly, the minimal distance d of the dual of C^\perp cannot be 1. Let $u = (p^k + 1)/2$. Then $\gcd(u, p^m - 1) = 1$ since k is even and m is odd. By the definition of C , the code C^\perp has a codeword of Hamming weight 2 if and only if there exist two elements $c_1, c_2 \in \text{GF}(3)^*$ and two distinct integers $0 \leq t_1 < t_2 \leq p^m - 2$ such that

$$\begin{cases} c_1(-\pi)^{t_1} + c_2(-\pi)^{t_2} = 0 \\ c_1\pi^{ut_1} + c_2\pi^{ut_2} = 0. \end{cases} \quad (20)$$

Note that $\gcd(u, p^m - 1) = 1$ and $t_1 \neq t_2$. It follows from the second equation of (20) that $c_1 = c_2$ and $t_2 = t_1 + (p^m - 1)/2$. Then the first equation becomes $2c_1(-\pi)^{t_1} = 0$, which is impossible. Thus the code C^\perp does not have a codeword of Hamming weight 2.

We now prove that C^\perp has no codeword of weight 3. Otherwise, there exist three elements c_1, c_2, c_3 in $\text{GF}(3)^*$ and three distinct integers $0 \leq t_1 < t_2 < t_3 \leq p^m - 2$ such that

$$\begin{cases} c_1(-\pi)^{t_1} + c_2(-\pi)^{t_2} + c_3(-\pi)^{t_3} = 0 \\ c_1\pi^{ut_1} + c_2\pi^{ut_2} + c_3\pi^{ut_3} = 0. \end{cases} \quad (21)$$

Due to symmetry it is sufficient to consider the following two cases.

Case A, when $c_1 = c_2 = c_3 = 1$: In this case, (21) becomes

$$\begin{cases} (-\pi)^{t_1} + (-\pi)^{t_2} + (-\pi)^{t_3} = 0 \\ \pi^{ut_1} + \pi^{ut_2} + \pi^{ut_3} = 0. \end{cases} \quad (22)$$

Let $x_i = \pi^{t_i}$ for $i = 1, 2, 3$. Then $x_1, x_2, x_3 \in \text{GF}(3^m)^*$ and are pairwise distinct. Without loss of generality, we only need to consider the following two subcases.

1) t_1 is even and t_2, t_3 are odd. In this subcase, we have

$$\begin{cases} x_1 - x_2 - x_3 = 0 \\ x_1^u + x_2^u + x_3^u = 0 \end{cases} \quad (23)$$

which yields

$$(x_2 + x_3)^u = -x_2^u - x_3^u.$$

Thus

$$(x_2 + x_3)^{2u} = (-x_2^u - x_3^u)^2$$

which leads to

$$x_2 x_3 \left(x_2^{(p^k-1)/2} - x_3^{(p^k-1)/2} \right)^2 = 0. \quad (24)$$

It then follows that $(x_3/x_2)^{p^k-1} = 1$. Note that $\gcd(m, k) = 1$, and x_2, x_3 are both nonsquare in $\text{GF}(3^m)$ since t_2, t_3 are odd. Thus $x_2 = x_3$. This is a contradiction to the fact that $x_2 \neq x_3$.

- 2) t_1, t_2 , and t_3 are even. Similarly, in this subcase, we can arrive at (24) in which x_2, x_3 are both squares in $\text{GF}(3^m)$ since t_2, t_3 are even. It then follows from $(x_3/x_2)^{p^k-1} = 1$ that $x_2 = x_3$. This is again a contradiction.

Case B, when $c_1 = c_2 = 1$ and $c_3 = -1$. The proof of this case is similar to Case A. We omit the details here.

Finally, by the Sphere Packing bound, the minimal distance $d \leq 4$. Hence $d = 4$. This completes the proof. ■

This subclass of ternary cyclic codes C^\perp are optimal in the sense that the minimum distance is maximal for any ternary linear code with length $3^m - 1$ and dimension $3^m - 1 - 2m$.

Example 4.2: Let $p = 3$ and $m = 3$, and $k = 2$. Then the code C^\perp is an optimal ternary cyclic code with parameters $[26, 20, 4]$ and generator polynomial $x^6 + 2x^5 + 2x^3 + x + 2$.

Example 4.3: Let $p = 3$ and $m = 5$, and $k = 4$. Then the code C^\perp is an optimal ternary cyclic code with parameters $[242, 10, 4]$ and generator polynomial $x^{10} + 2x^9 + x^8 + x^7 + x^6 + 2x^2 + 2$.

Example 4.4: Let $p = 3$ and $m = 7$, and $k = 6$. Then the code C^\perp is an optimal ternary cyclic code with parameters $[2186, 14, 4]$ and generator polynomial $x^{14} + 2x^{13} + x^{11} + 2x^{10} + x^6 + x^5 + 2$.

V. SUMMARY AND CONCLUDING REMARKS

In this paper, we presented a class of three-weight cyclic codes and determined their weight distributions. Some of the codes are optimal, and the duals of a subclass of the cyclic codes are also optimal.

While a lot of two-weight codes were discovered (see [1], [5], [6], [13], [10], [19]), only a small number of three-weight codes are known ([2], [5], [6], [8], [9]). It would be good if more three-weight codes are constructed, in view of their applications in association schemes and secret sharing schemes.

REFERENCES

- [1] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.*, vol. 18, pp. 97-122, 1986.
- [2] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," *Philips J. Res.*, vol. 39, pp. 143-152, 1984.
- [3] C. Carlet, C. Ding, and J. Yuan, "Linear codes from highly nonlinear functions and their secret sharing schemes," *IEEE Trans. Inform. Theory*, vol. 51, no. 6, pp. 2089-2102, 2005.
- [4] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. IT-21, no. 5, pp. 575-576, Sep. 1975.
- [5] C. Ding, Y. Liu, C. Ma, and L. Zeng, "The weight distributions of the duals of cyclic codes with two zeros," *IEEE Trans. Inform. Theory*, vol. 57, No. 12, pp. 8000-8006, Dec. 2011.
- [6] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Mathematics*, vol. 313, no. 4, pp. 434-446, 2013.
- [7] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields Appl.*, vol. no. 2, pp. 390-409, Apr. 2008.
- [8] T. Feng, "On cyclic codes of length $2^{2^t} - 1$ with two zeros whose dual codes have three weights," *Des. Codes Cryptogr.*, vol. 62, pp. 253-258, 2012.
- [9] G. McGuire, "On three weights in cyclic codes with two zeros," *Finite Fields Appl.*, vol. 10, no. 1, pp. 97-104, Jan. 2004.
- [10] W. M. Kantor, "Exponential numbers of two-weight codes, difference sets and symmetric designs," *Discrete Mathematics*, vol. 46, pp. 95-98, 1983.
- [11] A. Klapper, "Cross-correlations of quadratic form sequences in odd characteristic," *Des. Codes Cryptogr.*, vol. 3, no. 4, pp. 289-305, 1997.
- [12] Z. Liu and X.-W. Wu, "On a class of three-weight codes with cryptographic applications," In: *Proc. of the 2012 IEEE International Symposium on Information Theory*, pp. 2551-2555, 2012.
- [13] Z. Liu and X. Zeng, "On a kind of two-weight code," *European Journal of Combinatorics*, vol. 33, no. 6, pp. 1265-1272, Aug. 2012.
- [14] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," *IEEE Trans. Inform. Theory* vol. 54, no. 12, pp. 5345-5353, Dec. 2008.
- [15] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5332-5344, Dec. 2008.

- [16] C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, "The weight enumerator of a class of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 397–402, Jan. 2011.
- [17] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics, Vol. 20, Cambridge University Press, Cambridge, 1983.
- [18] F. MacWilliams and J. Seery, "The weight distributions of some minimal cyclic codes," *IEEE Trans. Inform. Theory*, vol. 27 no. 6, pp. 796–806, 1981.
- [19] B. Schmidt and C. White, "All two-weight irreducible cyclic codes," *Finite Fields Appl.*, vol. 8, pp. 1–17, 2002.
- [20] H. M. Trachtenberg, *On the crosscorrelation functions of maximal linear recurring sequences*, Ph.D. dissertation, Univ. South. Calif., Los Angels, 1970.
- [21] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 712–717, Feb. 2006.
- [22] B. Wang, C. Tang, Y. Qi, Y. X. Yang, and M. Xu, "The weight distributions of cyclic codes and elliptic curves," *IEEE Trans. Inform. Theory*, vol. 58, no. 12, pp. 7253–7259, Dec. 2012.
- [23] M. van der Vlugt, "On the weight hierarchy of irreducible cyclic codes," *J. Comb. Theory Ser. A*, vol. 71, no. 1, pp. 159–167, July 1995.